

ADMINISTRATIVE MESSAGE

ROUTINE

R 161957Z OCT 02 ZYB

FM DON CIO WASHINGTON DC//DONCIO//

CNO WASHINGTON DC//N6//

BT

UNCLAS

MSGID/GENADMIN/DON CIO WASHINGTON DC//

SUBJ/REMOTE ACCESS TO ENTERPRISE EMAIL FROM NON DOD COMPUTERS//

POC/LARRY PEMBERTON/LCDR USN/DON CIO/LOC:WASHINGTON DC

/TEL:703-601-0120//

RMKS/1. BACKGROUND. THIS INTERIM GUIDANCE IS THE RESULT OF THE 27 SEP 02 DON CIO HOSTED MEETING TO ADDRESS REMOTE ACCESS TO ENTERPRISE E-MAIL FROM PERSONALLY OWNED AND OTHER NON-DOD COMPUTERS. FINAL POLICY WILL BE PROMULGATED VIA SECNAVINST. DON CIO WILL ADDRESS REMOTE ACCESS TO LARGE DON APPLICATION SITES (E.G. TASK FORCE EXCEL) BY SEPCOR. THIS INTERIM GUIDANCE IS EFFECTIVE IMMEDIATELY.

2. POLICY: COMMANDING OFFICERS SHALL AUTHORIZE REMOTE ACCESS TO UNCLASSIFIED E-MAIL USING PERSONALLY OWNED AND OTHER NON-DOD COMPUTERS TO PERSONNEL WITH A VERIFIABLE NEED. PERSONNEL MUST COMPLY WITH APPROVED PROCEDURES AND COMPUTER CONFIGURATION REQUIREMENTS.

A. REQUESTING PERSONNEL SHALL:

(1) SUBMIT A REQUEST TO THEIR COMMANDING OFFICER FOR EACH

COMPUTER EXPECTED TO ACCESS A DON UNCLASSIFIED E-MAIL SYSTEM. EACH REQUEST SHALL INDICATE A VALID REQUIREMENT. CONVENIENCE ALONE IS NOT A VALID REQUIREMENT.

(2) SIGN A STATEMENT ACCEPTING RESPONSIBILITY FOR EACH APPROVED ACCESS.

(3) OBTAIN A DOD PUBLIC KEY INFRASTRUCTURE (PKI) IDENTITY CERTIFICATE, FOR AUTHENTICATION PURPOSES.

(4) HANDLE, STORE, MAINTAIN AND DESTROY ALL UNCLASSIFIED INFORMATION IN ACCORDANCE WITH DOD AND DON POLICIES.

(5) IMMEDIATELY NOTIFY THEIR COMMAND OF ANY INFORMATION LOSS, THEFT OR SUSPICIOUS BEHAVIOR OF THEIR SYSTEM(S).

(6) PROTECT THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF DON E-MAIL SYSTEMS AND INFORMATION AT ALL TIMES.

(7) COMPLETE ALL REQUIRED TRAINING.

(8) INSTALL, CONFIGURE, MAINTAIN AND UPDATE REQUIRED SECURITY SOFTWARE, HARDWARE, PKI CERTIFICATES AND CURRENT ANTI-VIRUS FILES BY UPDATING THEM AT LEAST WEEKLY OR WHEN PROMPTED.

(9) NOT USE PUBLIC ACCESS COMPUTERS, SUCH AS THOSE IN COLLEGE COMPUTER LABS, PUBLIC KIOSKS, LIBRARIES, ETC. TO ACCESS DON OR DOD UNCLASSIFIED E-MAIL ACCOUNTS.

(10) AT THE COMPLETION OF A SESSION:

(A) IF CONNECTED BY DIAL-UP MODEM OR DSL:

(1) CLOSE ALL DON E-MAIL FILES;

(2) CLEAR THE WEB BROWSER'S CACHE;

(3) EXIT AND CLOSE THE BROWSER

(B) IF CONNECTED BY CABLE MODEM:

- (1) CLOSE ALL DON E-MAIL FILES
- (2) CLEAR THE WEB BROWSER'S CACHE
- (3) EXIT AND CLOSE THE BROWSER
- (4) IMMEDIATELY TURN OFF THE COMPUTER. "SLEEP" AND "STANDBY" MODES ARE NOT ACCEPTABLE.

(11) USE A DOD PKI SOFTWARE CERTIFICATE FOR AUTHENTICATION TO REMOTE ACCESS SERVICES AND SHALL TRANSITION TO HARDWARE CERTIFICATES WHEN REQUIRED.

(12) INSTALL AND USE APPROVED ANTI-VIRUS PROTECTION AND PERSONAL FIREWALL SOFTWARE. APPROVED SOFTWARE IS AVAILABLE TO ALL DOD EMPLOYEES AT NO COST FROM THE DEFENSE INFORMATION SYSTEMS AGENCY (DISA) WEBSITE AT [HTTP://WWW.DISA.MIL/INFOSEC/IAWEB/DEFAULT.HTML](http://www.disa.mil/infosec/iaweb/default.html), UNDER THE DOD ENTERPRISE LICENSE. ADDITIONAL APPROVED PRODUCTS MAY BE FOUND ON THE NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)

VALIDATED PRODUCTS LIST AT
[HTTP://NIAP.NIST.GOV/NIAP/SERVICES/VALIDATED-PRODUCTS.HTML](http://niap.nist.gov/niap/services/validated-products.html).

(13) ENSURE THAT NO OTHER WIRELESS OR LAN CONNECTION EXISTS FOR THE DURATION OF THE SESSION. ANY OTHER EXISTING CONNECTIONS MUST BE DISABLED FOR THE DURATION OF THE SESSION.

B. COMMANDING OFFICERS SHALL:

(1) EVALUATE EACH REQUEST FOR VALIDITY AND APPROVE THOSE ESSENTIAL FOR MISSION ACCOMPLISHMENT.

(2) RETAIN ALL SIGNED STATEMENTS UNTIL MEMBER'S DEPARTURE. ELECTRONIC METHODS OF RETENTION ARE HIGHLY ENCOURAGED (I.E. SCANNED ELECTRONIC IMAGE, ETC.). DON WILL REVIEW ELECTRONIC METHODS OF DOCUMENT RETENTION AND SIGNING AND WILL RECOMMEND ALTERNATIVES.

(3) MAINTAIN A CURRENT LIST OF ALL AUTHORIZED USERS.

(4) ANNUALLY REVIEW APPROVALS.

(5) DISABLE ACCESS IMMEDIATELY UPON MEMBER'S DEPARTURE.

(6) ENSURE ALL REMOTE ACCESS TO E-MAIL IS MEDIATED THROUGH A
MANAGED ACCESS CONTROL POINT SUCH AS A REMOTE ACCESS SERVER IN A
DE-MILITARIZED ZONE (DMZ), AND SHALL ALWAYS USE ENCRYPTION TO
PROTECT THE CONFIDENTIALITY OF THE SESSION.

3. TECHNICAL ASSISTANCE CAN BE PROVIDED BY SPAWAR PMW-161 INFOSEC

TECHNICAL ASSISTANCE CENTER (ITAC). TOLL FREE: 1-800-304-4636

DSN: 588-5426/4286 COMM: 842-218-5426/4286.//

BT

#0310

NNNN

ACTION:

CIPRIANO, JOE (SMTP)

LAVOIE, MARK (SMTP)

THURMAN, MARSHA (SMTP)

OPP, DICK (SMTP)

MESSAGE CENTER, HELP DESK (SMTP)

FELDMANN, PEGGY (SMTP)